

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113

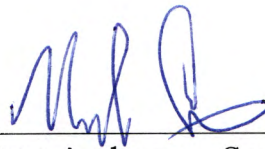
21-130-04

**REDACTED APPLICATION FOR
SEARCH AND SEIZURE
WARRANT**

I, Nathan Anderson, being duly sworn depose and say:

I am a Special Agent with the Homeland Security Investigations, and have reason to believe that on the property or premises as fully described in Attachment A, attached hereto and incorporated herein by reference, there is now concealed certain property, namely: that which is fully described in Attachment B, attached hereto and incorporated herein by reference, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of 18 U.S.C. §§ 2252A(a)(1) and 2252A(a)(5)(B) (involving the transportation and possession of child pornography).

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.



Nathan Anderson, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me, telephonically, on the 28th day of July,
2021, at Sioux Falls, South Dakota.



VERONICA L. DUFFY
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113

21-130-04

**REDACTED SEARCH AND
SEIZURE WARRANT**

TO: ANY AUTHORIZED LAW ENFORCEMENT OFFICER

An application by a federal law enforcement officer or an attorney for the government requests the search of the following property more fully described in Attachment A, attached hereto and incorporated herein by reference.

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the property described above, and that such search will reveal evidence of violations of 18 U.S.C. § 2252A (certain activities relating to child pornography), which is more fully described in Attachment B, attached hereto and incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before

August 11, 2021 (not to exceed 14 days)

☒ in the daytime - 6:00 a.m. to 10:00 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the undersigned Judge.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized,

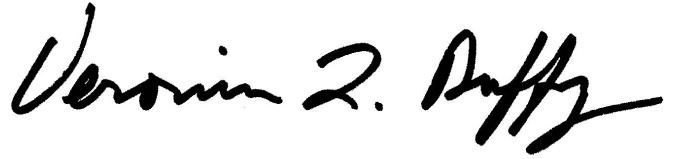
☐ for _____ days (*not to exceed 30*).

☐ until, the facts justifying, the later specific date of _____.

July 28, 2021 at 2:55 p.m. CDT

Date and Time Issued Telephonically

at Sioux Falls, South Dakota

A handwritten signature in black ink, reading "Veronica L. Duffy". The signature is written in a cursive, flowing style with a large initial 'V' and a long, sweeping underline.

VERONICA L. DUFFY

United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113
21-130-04 **REDACTED RETURN**

Date and time warrant executed: _____

Copy of warrant and inventory left with: _____

Inventory made in the presence of: _____

Inventory of the property taken and name of any person(s) seized (attach additional sheets, if necessary):

CERTIFICATION
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.
<div style="text-align: right;">_____ Nathan Anderson, Special Agent Homeland Security Investigations</div>

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113

21-130-04

REDACTED ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The warrant applies to the contents and information associated with the Google accounts [REDACTED]@gmail.com and [REDACTED]@gmail.com, known to be stored at the premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94403.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113
21-130-04 **REDACTED ATTACHMENT B**

DESCRIPTION OF PROPERTY TO BE SEIZED

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Google, Inc. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A [REDACTED]

[REDACTED]:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Google, Inc. accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails "invites" sent or received via Google, Inc., and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Google, Inc. and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the accounts associated with the Google, Inc. accounts [REDACTED]@gmail.com and [REDACTED]@gmail.com in furtherance of all aforementioned crimes.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to Special Agent Nathan Anderson at the address 2708 North 1st Avenue Sioux Falls, SD 57104, or by email to Nathan.J.Anderson@ice.dhs.gov.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding:

21-130-04

No. 21-mj-113

**REDACTED AFFIDAVIT IN
SUPPORT OF SEARCH AND
SEIZURE WARRANT**

STATE OF SOUTH DAKOTA)
 :SS
COUNTY OF MINNEHAHA)

I, Nathan Anderson, being duly sworn on oath, depose and say:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Sioux Falls, South Dakota, and have been duly employed in this position since March 2020. I am a graduate of the Criminal Investigator Training Program (CITP) and HSI Special Agent Training Program (HSISAT) at the Federal Law Enforcement Training Center (FLETC). I have received specialized training pertaining to conducting criminal investigations, immigration and customs laws, investigative techniques, searching databases, conducting interviews, executing search warrants, and making arrests with respect to criminal violations of United States Code.

2. I have investigated and have assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of 18 U.S.C. §§ 2251, 2252, and 2252A, involving violations of law involving child pornography and 18 U.S.C. § 2422(b), enticement of a minor using the internet. During my law enforcement career, I have become familiar with the 'modus operandi of persons involved in the illegal production, distribution, and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive, and possess child pornography.

APPLICABLE LAW

3. Title 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution,

possessing, or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct, or produced using a minor engaged in such conduct, when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

4. Title 18 U.S.C. § 2252A(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

RELEVANT ELECTRONIC AND WIRE COMMUNICATION STATUTES

5. The relevant federal statutes involved in the disclosure of customer communication records for the requested data in the **Subject Accounts** are as follows:

- a. 18 U.S.C. § 2703(a) provides, in part: “A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction.”
- b. 18 U.S.C. § 2703(b)(1) provides, in part, that a governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction.
- c. 18 U.S.C. § 2703(c)(1) provides, in part, that a governmental entity may require a provider of electronic communication service or remote computing service to disclose non-content subscriber or customer information when the governmental entity obtains a warrant issued using the procedures

described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction, although that is not the only means by which the government can obtain subscriber information.

- d. 18 U.S.C. § 2510(12) defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce,” with certain exceptions not applicable here.
- e. 18 U.S.C. § 2510(17) defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof” and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”
- f. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A), and 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. See 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

PURPOSE OF AFFIDAVIT

6. I submit this affidavit in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(c)(1)(A) for information about the Google email address, “**██████████@gmail.com**” and “**██████████@gmail.com**” (the “**Subject Accounts**”) as described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and 2252A(a)(5)(B) (involving the transportation and possession of child pornography) as described in Attachment B.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, a review of records related to this investigation, communications with others who

have knowledge of the events and circumstances described herein, and information gained through my training and experience.

8. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the **Subject Accounts** constitutes evidence or instrumentalities of criminal violations Title 18, U.S.C. § 2252A(a)(1) - Knowingly mail, ship, or transport any child pornography and Title 18, U.S.C. § 2252A(a)(5)(B) - Knowingly possess or access with intent to view child pornography.

SUMMARY OF INVESTIGATION

9. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of United States Code are located within the **Subject Accounts**.

10. On [REDACTED]

11. On [REDACTED]

12. *Image file name:* "[REDACTED]"

a. *Description:* [REDACTED]

13. I also reviewed [REDACTED]

14. Video file name: " [REDACTED] "

Description:

15. On [REDACTED]

_____@gmail.com

- Name: [REDACTED]
- Recovery Email: [REDACTED]@gmail.com
- Recovery Phone: [REDACTED]
- Billing Name: [REDACTED]
- Billing Address: [REDACTED], Sioux Falls, SD 57108
- Recovery Phone: [REDACTED]

[REDACTED]@gmail.com

- Name: [REDACTED]
- Recovery Email: [REDACTED]@gmail.com
- Recovery Phone: [REDACTED]
- Billing Name: [REDACTED]

- Billing Address: [REDACTED], Sioux Falls, SD 57108

16. On [REDACTED]

- Full name: [REDACTED]
- Date of birth: [REDACTED], 2000
- Physical address: [REDACTED], Sioux Falls, SD, 57108
- Driver's license number: [REDACTED]
- Current registered vehicle: None
- Last known employer: [REDACTED]

17. On [REDACTED]

18. [REDACTED]

19. [REDACTED]

- Account Number: [REDACTED]
- Start Date Time: [REDACTED]
- End Date Time: [REDACTED]
- Account holder name: [REDACTED]
- Account holder address: [REDACTED], Sioux Falls, SD, 57108
- Home phone: [REDACTED]

20. Further records checks conducted on [REDACTED], Sioux Falls, SD, indicate [REDACTED].

21. Based on my training and experience, I know that individuals [REDACTED]

INFORMATION REGARDING NCMEC

22. National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further their mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Programs. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Programs available to law enforcement and uses this information to help identify trends and create child safety and prevention messages. As a national clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement, and the public in a combined effort to reduce online child sexual abuse images. NCMEC does not act in the capacity of or under the direction or control of the government or any law enforcement agency. NCMEC does not independently investigate and cannot verify the accuracy of the information submitted by reporting parties

INFORMATION REGARDING GOOGLE, INC.

23. In my training and experience, I have learned that Google, Inc. provides a variety of online services, including electronic mail ("email") access, to the general public. Subscribers obtain an account by registering with Gmail, Google, Inc.'s free, web-based email service. During the registration process, Gmail asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail subscribers and information concerning subscribers and their use of Gmail services, such as account access information, email transaction information, and account application information).

24. In general, an email that is sent to a Gmail subscriber is stored in the subscriber's "mailbox" on Google, Inc. servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc. servers indefinitely.

25. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google, Inc. servers, and then

transmitted to its end destination. Google, Inc. often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google, Inc. server, or terminates the email account, the email can remain on the system indefinitely.

26. A Google subscriber can also store files, including emails, address books, contact, or buddy lists, pictures, and other files, on servers maintained and/or owned by Google, Inc.

27. Subscribers to Gmail might not store on their home computers copies of the emails stored in their Gmail email account. This is particularly true when they access their Gmail account through the web, or if they do not wish to maintain particular emails or files in their residence.

28. In general, email providers like Google, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and for paying subscribers, means and source of payment (including any credit or bank account number).

29. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Gmail website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

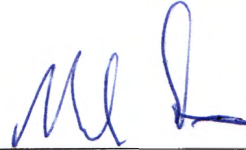
30. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

31. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files

32. I know from my training and experience that Oath preserves the content of the accounts that have been flagged, or at the request of a law enforcement agency preservation request.

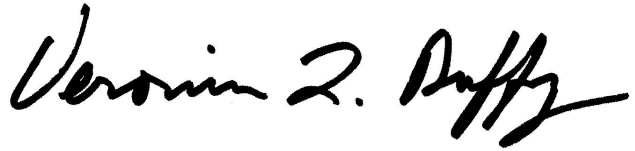
CONCLUSION

33. Based on the foregoing, I have probable cause to believe that the user of the **Subject Accounts**, believed to be [REDACTED], knowingly and unlawfully transported and possessed child pornography, and that contraband and evidence of those offenses, as more fully described in Attachment B, are presently contained in the **Subject Accounts**. I therefore request that the Court issue a warrant authorizing a search of the **Subject Accounts** described in Attachment A for the items listed in Attachment B and the examination and seizure of any such items found.



Nathan Anderson, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me, telephonically, on this 28th day of
July, 2021, at Sioux Falls, South Dakota.



VERONICA L. DUFFY
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113

21-130-04

REDACTED ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The warrant applies to the contents and information associated with the Google accounts [REDACTED]@gmail.com and [REDACTED]@gmail.com, known to be stored at the premises controlled by Google, Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94403.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search Regarding: No. 21-mj-113

21-130-04

REDACTED ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEIZED

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Google, Inc. or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A [REDACTED]

[REDACTED]:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Google, Inc. accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails "invites" sent or received via Google, Inc., and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Google, Inc. and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the accounts associated with the Google, Inc. accounts [REDACTED]@gmail.com and [REDACTED]@gmail.com in furtherance of all aforementioned crimes.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to Special Agent Nathan Anderson at the address 2708 North 1st Avenue Sioux Falls, SD 57104, or by email to Nathan.J.Anderson@ice.dhs.gov.